TMA Privacy Act Refresher Training

TMA Privacy Office

HEALTH AFFAIRS

TRICARE Management Activity

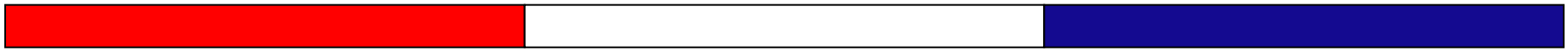
Purpose

- Provide an overview of Privacy Act and Department of Defense (DoD) Privacy Program
- Understand privacy terms
- Review DoD Privacy Program requirements
- Be familiar with recent privacy updates
- Know how to report a privacy data breach
- Be able to implement Best Practices for protecting Personally Identifiable Information (PII)

Objectives

- Upon completion of this course you will be able to:
  - Discuss updates to DoD Regulation 5400.11-R, “DoD Privacy Program”
  - Define privacy terms
  - Explain the DoD Privacy Program requirements
  - Understand the impact of privacy data breaches
  - Know the data breach reporting timeline

Privacy Act and DoD Privacy Program



Privacy Act and DoD Privacy Program

- Privacy Act of 1974, as amended (5 U.S.C. 552a)
- DoD Regulation 5400.11-R, “DoD Privacy Program,” May 14, 2007

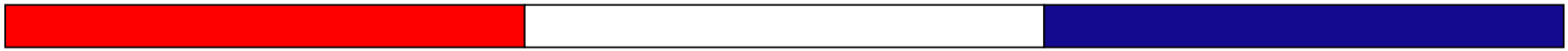
Privacy Act of 1974

- The purpose of the Privacy Act is to:
  - Safeguard individual privacy of information contained in Federal records
  - Provide individuals access and amendment rights to records concerning them which are maintained by Federal agencies
  - Put in proper balance individual privacy with the Government's need to maintain information about individuals
- Privacy Act requires each Agency to:
  - Establish rules of conduct for all persons involved with Systems of Records
  - Train personnel about the established rules

DoD Privacy Program

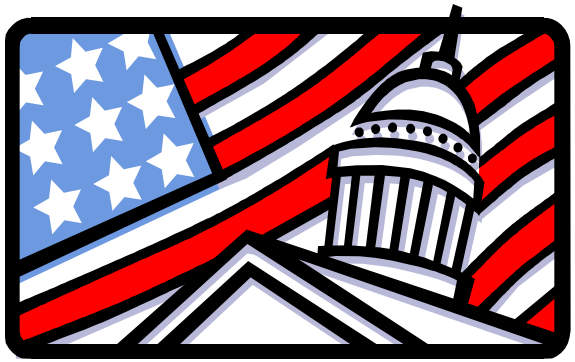
- DoD Regulation 5400.11-R, “DoD Privacy Program,” May 14, 2007 addresses:
  - Collection of PII
  - Individual Access
  - Disclosure of PII
  - System of Records
  - Computer Matching Procedures
  - Training Requirements
  - Privacy Act Violations
  - Reports and Inspections
  - Publication Requirements

DoD Privacy Program Terms



DoD Privacy Program Terms

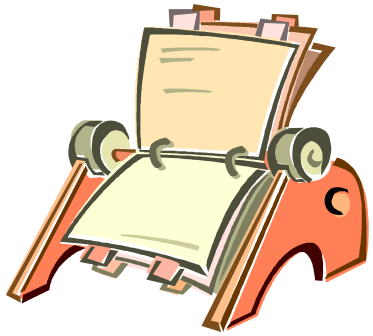
- Personally Identifiable Information (PII)
- Individual Access
- Disclosure of PII
- System of Records
- System of Records Notice (SORN)
- Computer Matching
- Lost, Stolen, or Compromised Information



DoD Privacy Program Terms

Personally Identifiable Information

- The Privacy Act defines Personally Identifiable Information (PII) as “information which can be used to distinguish or trace an individual’s identity.”



DoD Privacy Program Terms

Personally Identifiable Information

- PII includes:
  - Name
  - Social Security number
  - Age
  - Date and place of birth
  - Mother's maiden name
  - Biometric records
  - Military Rank or Civilian Grade
  - Marital status
  - Race
  - Salary
  - Home/office phone numbers
  - Other personal information which is linked to a specific individual

DoD Privacy Program Terms

Individual Access

- **Individual** is a living person who is a citizen of the United States or an alien lawfully admitted for permanent residence which includes:
  - The parent of a minor or the legal guardian of any individual who may also act on behalf of an individual
  - Members of the U.S. Armed Forces
- **Individual Access** is access to information pertaining to the individual by the individual or his or her designated agent or legal guardian

DoD Privacy Program Terms

Disclosure of Personally Identifiable Information

- **Disclosure** is the transfer of any PII from a System of Records
  - By any means of communication (such as oral, written, electronic, mechanical, or actual review)
  - To any person, private entity, or Government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian

DoD Privacy Program Terms

System of Records

- **System of Records** is a group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number or symbol that is unique to the individual

DoD Privacy Program Terms

System of Records Notice

- **System of Records Notice (SORN)**
  - Advance public notice must be published 40 days before an Executive Agency begins to collect personal information for a new System of Records
    - 30 days for public comment and 10 extra days for OMB and Congress to comment
  - Publication in the Federal Register is required to provide an opportunity for interested persons to comment

DoD Privacy Program Terms

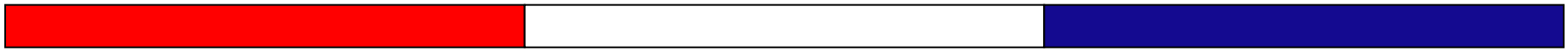
Computer Matching

- **Computer Matching** is the computerized comparison of two or more automated Systems of Records with non-Federal records
- **Computer Matching Programs** for covered systems can use records from Federal personnel or payroll Systems of Records
- Computer Matching is most often used to determine the eligibility for Federal benefits

Lost, Stolen, or Compromised Information

- **Lost, Stolen, or Compromised Information** is:
  - Actual or possible loss of control, unauthorized disclosure, or unauthorized access of PII
  - Where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected
  - Also called a breach

DoD Privacy Program Requirements



DoD Privacy Program Requirements

- Collection of PII
- Individual Access
- Disclosure of PII
- System of Records
- Computer Matching Procedures
- Training Requirements
- Privacy Act Violations
- Reports and Inspections
- Publication Requirements

Collection of Personally Identifiable Information

- PII should be collected directly from the individual, or
- In some instances, PII may be collected from Third Parties, such as to verify information for security clearances or employment
- Individuals have the right to withhold their Social Security numbers
- An individual must be given a Privacy Act statement:
  - Whenever his or her PII is to be included in a System of Records
  - Specifying whether furnishing the requested PII is mandatory or voluntary

Individual Access

- Individual Access is allowed:
  - For individuals, even minors, who make formal requests to access their records that are maintained in a System of Records
  - After the individual's identity is verified
  - To the original records or an exact copy of the original
    - If the requested records are illegible, incomplete, or partially exempt; copy the record as it is
    - If access to such records would neither have an adverse effect on the mental or physical health of the individual nor result in harm to a third party
  - Within 20 working days after receipt of the request; if this is not possible, the individual must be notified

Denial of Individual Access

- Denial of Individual Access:
  - May occur if there are civil proceedings pending or the record contains classified information
  - Requires a written formal notification to the individual for formal denials
  - Allows for appeals to denials that must be processed within 30 days of receipt

Amendments and Copying Fees

- Amendment of Records:
  - Allows individuals to review and request corrections to their PII
  - Allows individual to request amendments to their records contained in a System of Records
  - Requires that a written acknowledgement of the request to amend be provided to the individual within 10 working days of receipt of the request
- Reproduction Fees are only allowed for the direct cost of the reproduction

Disclosure of Personally Identifiable Information

- Disclosures may be made in certain instances:
  - To Third Parties, DoD Components, Law Enforcement, and Commercial Enterprises
  - For Established Routine Uses, Statistical Research or Reporting, Emergencies, and Court Orders
- Validation of identity is required before disclosing PII to the entity
- Disclosure Accounting must be maintained and provided upon request

DoD Privacy Program Requirements

Systems of Records

- Systems of Records must:
  - Provide for retrieval of records by the name of an individual or some other personal identifier
  - Contain only PII that is relevant and necessary to accomplish a purpose of the DoD Component
  - Maintain accurate, timely, and complete records
  - Allow sharing with Government contractors
  - Maintain Minimum Standards and Records Disposal policies and procedures
  - Require notifying the individual when information is lost, stolen, or compromised

Systems of Records and Contractors

- DoD contractors are required to maintain a System of Records including the collection, use, and dissemination of records on behalf of the contracting DoD Component
- Contractors (and their employees), sub-contractors, and volunteers who maintain a System of Records shall be considered employees of the contracting DoD Component for the purposes of the **criminal penalties** of the Privacy Act

DoD Privacy Program Requirements

Computer Matching Procedures

- Computer Matching Program Procedures include:
  - Computer Matching Publication and Review Requirements that:
    - Identify the Systems of Records that will be used in a match
    - Require disclosure of records outside the DoD
    - Establish the routine use
    - Meet the publication and review requirements before any disclosures are made
  - Computer Matching Agreements require:
    - A Memorandum of Understanding (MOU) if a match is to be conducted internally within the DoD
    - A Cost-Benefit Analysis of the computer matching program be conducted before beginning the match

DoD Privacy Program Requirements

Training Requirements

- DoD Privacy Program training requirements must be:
  - Job-specific and related to an individual's responsibilities
  - A prerequisite **before** an employee, manager, or contractor is permitted to access DoD systems
  - Mandatory for affected DoD military personnel, employees, managers, and contractors and business partners
- Four different trainings are required:
  - Orientation
  - Specialized
  - Management
  - Privacy Act Systems of Records

Privacy Act Violations

- The Privacy Act Violations' section addresses:
  - Civil Actions
  - Criminal Penalties
  - Administrative Remedies
  - Civil Remedies
  - Lost, Stolen, or Compromised Information

Civil Actions and Criminal Penalties

- **Civil Actions** allow individuals to file civil suits against DoD Components
- **Criminal Penalties** allow that any official or employee may be found guilty of a misdemeanor and fined not more than $5,000 per incident, if he or she:
  - Willfully disclosed information from a System of Records
  - Maintained a System of Records without publishing the required Public Notice in the Federal Register
  - Knowingly and willfully requested or obtained access to any record concerning another individual under false pretenses

Administrative and Civil Remedies

- **Administrative Remedies** allow DoD employees to file legitimate complaints against the DoD
- **Civil Remedies** allow specific remedial actions, such as payment for damages, court costs, and attorney's fees

Lost, Stolen, or Compromised Information

- Whenever there is lost, stolen, or compromised PII, DoD Components are required to:
  - Notify affected individual(s) of the loss, theft, or compromise
  - Specify timelines for follow-up and reporting
  - Outline procedures for resolving the issue

DoD Privacy Program Requirements

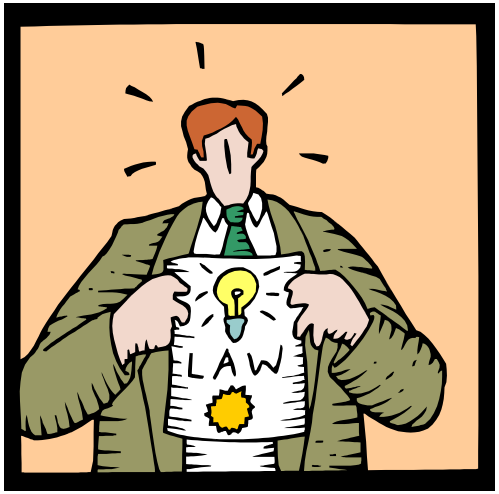
Reports and Inspections

- The Defense Privacy Office establishes the requirements for DoD Privacy Reports with the DoD Components providing the data
- Privacy Act Inspections are conducted by DoD Component inspectors
- Inspection Reports include the overall assets of the DoD Component Privacy Program

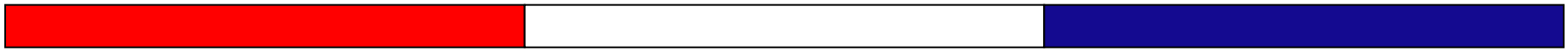
DoD Privacy Program Requirements

Publication Requirements

- Four types of documents must be published in the *Federal Register*:
  - DoD Component Privacy Procedural Rules
  - DoD Component Exemption Rules
  - System Notices
  - Computer Match Notices



DoD Privacy Program Update



DoD Privacy Program Update

- The Office of the Secretary of Defense (OSD) Memorandum 15041-07, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” September 21, 2007
- Updates affect DoD compliance with Office of Management and Budget (OMB) A-130 and Federal Information Security Management Act (FISMA) privacy reporting

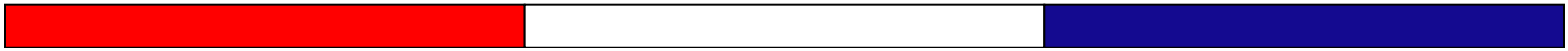
DoD Compliance with OMB A-130

- DoD Directive 5400.11 and DoD 5400.11-R are being revised to comply with the OMB Circular A-130, to require DoD to:
  - Biennially review each Privacy Act System of Records Notice (SORN) to ensure that it accurately describes the System of Records (SOR)
  - Review all systems that contain PII, whether or not they qualify as Privacy Act SOR, to determine whether the records are accurate, relevant, timely, and complete

FISMA Privacy Reporting Updated

- Instructions for FISMA privacy reporting are being updated to require DoD Components to:
  - Confirm there is an established, or are in the process of establishing, PII review plans
  - Provide a schedule to be updated periodically to review their holdings following the initial review to include:
    - Identifying all Components' automated systems containing PII in the DoD Information Technology Portfolio Repository (DITPR)
    - Periodically reviewing and update PII holdings at least once every 2 years
    - Revising FISMA reporting and annually reporting to the Defense Privacy Office

Privacy Data Breaches



Privacy Data Breaches

- What are Privacy Data Breaches?
- TMA Reporting Requirements
- TMA Contact Information
- Reporting TMA Privacy Breaches
- Privacy Data Breaches Increasing
  - Breach News Flash, July 16, 2007
  - Breach News Flash, July 23, 2007

What are Privacy Data Breaches?

- **Privacy Data Breaches are Inappropriate Disclosures** that may:
  - Be lost, stolen, or compromised PII
  - Be intentional or accidental
  - Affect high-risk or low-risk PII
  - Be found immediately or after a delay
  - Also be referred to as a breach

TMA Reporting Requirements

- Notify the U.S. CERT Incident Reporting System within 1 hour of the determination an incident occurred
- Notify TMA Privacy Office and if applicable, the Contracting Officer, within 1 hour of the determination an incident occurred (PrivacyOfficerMail@tma.osd.mil)
- Complete and submit electronic TMA Breach Report within 48 hours of the determination an incident occurred to PrivacyOfficerMail@tma.osd.mil

TMA Contact Information

- To report TMA privacy breaches contact:
  - Leslie Shaffer, Director, TMA Privacy Office
    - 703-681-7500
    - PrivacyOfficerMail@tma.osd.mil

Privacy Data Breaches Increasing

- The **U. S**. **CERT**, the Federally-funded research and development center, reports security incidents have exploded at an annual rate of 94% over just the last three years
- The **Privacy Rights Clearinghouse** has reported that more than 100 million records were involved in a data breach between 2005 and 2007
- Read the following *News Flashes* of two recent incidents that occurred within eight days of each other

Breach News Flash – July 16, 2007

- "TSA Storage Device Missing from Headquarters"

  "Authorities realized in May a storage device was missing from TSA headquarters. The drive contained historical payroll data, Social Security numbers, dates of birth, addresses, time and leave data, bank account routing information, and details about financial allotments and deductions."

  Source: www.privacyrights.org, July 16, 2007

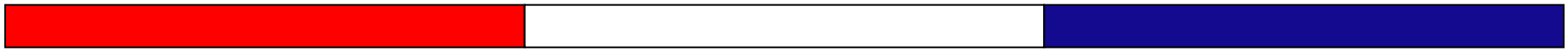
Breach News Flash – July 23, 2007

- "Health Data on Service Members Sent Without Encryption"

"A large government contractor handling sensitive health information for over 800,000 U. S. Service members and their families acknowledged that some of its employees sent unencrypted data—such as medical appointments, treatments, and diagnoses—across the internet. Air Force investigations are probing the security breach at the contractor site in San Diego …"

Source: www.gigalaw.com, July 23, 2007

Conclusion



Best Practices

- Special Handling for Privacy Data
- Best Practices to Protect PII

Special Handling for Privacy Data

- Special handling required to protect privacy data or sensitive data includes:
  - **Labeling** Personally Identifiable Information (PII) as “For Official Use Only” (FOUO)
  - **Accessing** only what is necessary to complete a work-related duty or job
  - **Disclosing** verbal, paper, and electronic PII only within and between authorized entities to conduct official business
  - **Transmitting** PII between facilities or through e-mail
  - **Transporting** PII physically between approved locations and with prior authorizations
  - **Storing** PII after formal approval for transfer to a storage site
  - **Destroying** PII in accordance with the Administrative Instruction (AI)-15

Best Practices to Protect Personally Identifiable Information

- **Best Practices** to protect PII are to:
  - Develop and implement clear policies and procedures
  - Collect the minimum amount of PII and for the least amount of time
  - Classify PII in records' systems according to sensitivity
  - Require contractors who handle PII to follow DoD security policies and procedures
  - Dispose of records and equipment containing PII in a secure manner
  - Provide ongoing privacy data protection training
  - Report breaches immediately

Summary

- Having completed this training you should now be able to:
  - Discuss updates to DoD Regulation 5400.11-R, “DoD Privacy Program”
  - Define privacy terms
  - Explain the DoD Privacy Program requirements
  - Understand the impact of privacy data breaches
  - Know the data breach reporting timeline

Resources

Resources

- Privacy Act of 1974, as amended (5 U.S.C. 552a)
- DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007
- DoD Regulation 5400.11-R, “DoD Privacy Program,” May 14, 2007
- DoD 6025.18-R, “DoD Health Information Privacy Regulation,” January 24, 2003
- DoD 8580.02-R, “DoD Health Information Security Regulation,” July 12, 2007
- DoD Instruction 8500.2, “DoD Information Assurance Implementation,” February 6, 2003
- DoD Memorandum, “DoD Guidance on Protecting Personally Identifiable Information (PII),” August 18, 2006

Resources (continued)

- U.S. CERT: https://forms.us-cert.gov/report/
- "TSA Storage Device Missing from Headquarters," www.privacyrights.org, July 16, 2007
- "Health Data on Service Members Sent Without Encryption," http://www.gigalaw.com, July 23, 2007
- TRICARE Management Activity: http://www.tricare.osd.mil
- TMA Privacy Office E-News, to subscribe: http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm
- Protected Health Information Management Tool (PHIMT) Support for tool-related questions: EIDS@mhs-helpdesk.com
- TMA Privacy Office for subject matter questions: privacymail@tma.osd.mil

Print Your Certificate

http://www.usuhs.mil/oac/privactcertificate.doc